TraceFind.info

OSINT EMAIL INVESTIGATION PLATFORM

OSINT INTELLIGENCE REPORT

Email Footprint Assessment

Cross-referenced exposure analysis for the subject email address, including breach intelligence, online presence, and domain validity.

SUBJECT

test@gmail.com

CASE ID	GENERATED
TF-20260819-BFD10F	Aug 19, 2026 · 20:05 UTC

01 — Overview

Executive Summary

At-a-glance assessment of the subject's online exposure based on aggregated open-source intelligence sources.

EXPOSURE LEVEL

HIGH

Computed risk classification

DATA BREACHES

8

156,260,076 records exposed in total

DIGITAL FOOTPRINT

3

Platforms with a registered account

DOMAIN STATUS

VALID

MX / deliverability check

Investigation summary: the subject's email domain is operational; the address appears in **8** known data breach(es); and an account presence was identified on **3** online platform(s).

02 — Domain

Domain Validation

Verifies that the email's domain has valid DNS / MX records and is capable of receiving mail at the time of analysis.

✓ **Domain is valid and resolvable.**

03 — Exposure

Data Breach Intelligence

The subject was identified in **8** separate breach event(s), affecting a cumulative **156,260,076** records.

Adobe

VERIFIED

adobe.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Oct 04, 2013	152,445,165	4

EXPOSED FIELDS: Email addresses, Password hints, Passwords, Usernames

In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Gawker

VERIFIED

gawker.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Dec 11, 2010	1,247,574	3

EXPOSED FIELDS: Email addresses, Passwords, Usernames

In December 2010, Gawker was attacked by the hacker collective "Gnosis" in retaliation for what was reported to be a feud between Gawker and 4Chan. Information about Gawkers 1.3M users was published along with the data from Gawker's other web presences including Gizmodo and Lifehacker. Due to the prevalence of password reuse, many victims of the breach then had their Twitter accounts compromised to send Acai berry spam.

Stratfor

VERIFIED

stratfor.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Dec 24, 2011	859,777	7

EXPOSED FIELDS: Credit cards, Email addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames

In December 2011, "Anonymous" attacked the global intelligence company known as "Stratfor" and consequently disclosed a veritable treasure trove of data including hundreds of gigabytes of email and tens of thousands of credit card details which were promptly used by the attackers to make charitable donations (among other uses). The breach also included 860,000 user accounts complete with email address, time zone, some internal system data and MD5 hashed passwords with no salt.

Manga Traders

VERIFIED

mangatraders.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Jun 09, 2014	855,249	2

EXPOSED FIELDS: Email addresses, Passwords

In June 2014, the Manga trading website Mangatraders.com had the usernames and passwords of over 900k users leaked on the internet (approximately 855k of the emails were unique). The passwords were weakly hashed with a single iteration of MD5 leaving them vulnerable to being easily cracked.

Yahoo

VERIFIED

yahoo.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Jul 11, 2012	453,427	2

EXPOSED FIELDS: Email addresses, Passwords

In July 2012, Yahoo! had their online publishing service "Voices" compromised via a SQL injection attack. The breach resulted in the disclosure of nearly half a million usernames and passwords stored in plain text. The breach showed that of the compromised accounts, a staggering 59% of people who also had accounts in the Sony breach reused their passwords across both services.

Win7Vista Forum

VERIFIED

win7vista.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Sep 03, 2013	202,683	8

EXPOSED FIELDS: Email addresses, Instant messenger identities, IP addresses, Names, Passwords, Private messages, Usernames, Website activity

In September 2013, the Win7Vista Windows forum (since renamed to the "Beyond Windows 9" forum) was hacked and later had its internal database dumped. The dump included over 200k members' personal information and other internal data extracted from the forum.

Boxee

VERIFIED

forums.boxee.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Mar 29, 2014	158,093	10

EXPOSED FIELDS: Dates of birth, Email addresses, Geographic locations, Historical passwords, Instant messenger identities, IP addresses, Passwords, Private messages, User website URLs, Usernames

In March 2014, the home theatre PC software maker Boxee had their forums compromised in an attack. The attackers obtained the entire vBulletin MySQL database and promptly posted it for download on the Boxee forum itself. The data included 160k users, password histories, private messages and a variety of other data exposed across nearly 200 publicly exposed tables.

Pixel Federation

VERIFIED

pixelfederation.com

BREACH DATE	RECORDS EXPOSED	DATA TYPES
Dec 04, 2013	38,108	2

EXPOSED FIELDS: Email addresses, Passwords

In December 2013, a breach of the web-based game community based in Slovakia exposed over 38,000 accounts which were promptly posted online. The breach included email addresses and unsalted MD5 hashed passwords, many of which were easily converted back to plain text.

04 — Identity

Google Account Profile

Public profile metadata recovered from the subject's linked Google (Gaia) account.

Google Profile

GAIA ID 109697950876659362233

ENRICHED

Last Profile Edit	2025/01/11 16:11:48 (UTC)
Enterprise User	No
Profile Page	https://www.google.com/maps/contrib/109697950876659362233/reviews
Probable Location	Troisdorf, Deutschland · confidence: Low

ACTIVITY STATISTICS

2	2	5	0
Reviews	Ratings	Average Rating	Photos

05 — Footprint

Online Account Presence

The subject email is registered on **3** platform(s); **2** returned additional profile metadata.

Adobe

https://adobe.com

ENRICHED

Account Type	individual
Avatar	
Auth Methods	Otp, Facebook
Profile	https://account.adobe.com/profile

Github

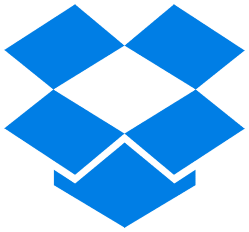
https://github.com

FOUND

Trello

https://trello.com

ENRICHED

Full Name	Test User
Username	testuser
Avatar	
Confirmed	Yes
Profile Page	https://trello.com/testuser